

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
8. Februar 2001 (08.02.2001)

PCT

(10) Internationale Veröffentlichungsnummer
WO 01/09830 A1

- (51) Internationale Patentklassifikation: G06K 19/14 (71) Anmelder und
(72) Erfinder: KIM, In-Ho (DE/DE); Am Teltower Damm
168, D-14167 Berlin (DE); MENZ, Alexander-Michael
(DE/DE); Viktoriast. 8, D-12105 Berlin (DE).
- (21) Internationales Aktenzeichen: PCT/DE00/02606 (74) Anwalt: MEISSNER, P. E.; Meissner & Meissner, Ho-
henzollerndamm 89, D-14199 Berlin (DE).
- (22) Internationales Anmeldedatum: 31. Juli 2000 (31.07.2000)
- (25) Einreichungssprache: Deutsch (81) Bestimmungsstaaten (national): CN, JP, KR, US.
- (26) Veröffentlichungssprache: Deutsch (84) Bestimmungsstaaten (regional): europäisches Patent (AT,
BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC,
NL, PT, SE).
- (30) Angaben zur Priorität: 199 36 998,4 2. August 1999 (02.08.1999) DE Veröffentlicht:
100 11 824,0 9. März 2000 (09.03.2000) DE — Mit internationalem Recherchenbericht.

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR ARCHIVING DOCUMENTS WITH A DIGITAL SIGNATURE ON PAPER OR SIMILAR MATERI-
ALS

(54) Bezeichnung: VERFAHREN ZUR ARCHIVIERUNG DIGITAL SIGNIERTER DOKUMENTE AUF PAPIER UND ÄHNLI-
CHEN MATERIALIEN

(57) Abstract: The invention relates to a method for representing electronic documents with a digital signature in a printed form and for verifying said signature from the printed form.

(57) Zusammenfassung: Verfahren zur Darstellung digital signierter elektronischer Dokumente in gedruckter Form und zur Verifikation der Signatur aus der gedruckten Form.



WO 01/09830 A1

Beispiel-Versicherungen AG

Beispielhausen, 1. Januar 2001

Auslandsreise-Krankenversicherung

Sehr geehrter Herr Mustermann,

hiermit senden wir Ihnen die Versicherungsunterlagen für Ihre Reisekrankenversicherung zu. Bitte machen Sie einen Ausdruck von diesem Dokument und verwahren ihn sorgfältig. Er ist Ihr Versicherungsnachweis.

Versicherungsnummer: RK 45 863 221 009
Versicherungsnehmer: Matthias Mustermann
Geburtsdatum: 01.01.1970
Anschrift: Hauptstraße 10
12345 Musterstadt

Tarif: Reisekrankenversicherung RK 45
Versichert sind alle Auslandsaufenthalte des Versicherungsnehmers im Versicherungszeitraum mit einer Dauer von jeweils maximal 45 Tagen.

Versicherungszeitraum: 01.01.2001-31.12.2001
Versicherungsprämie: 20.00 DM (10,73 EUR)

Die Versicherungsprämie wird in den nächsten Tagen von Ihrem Konto abgebucht.

Seite 1 von 1

Dieses Dokument ist digital signiert.

WO 01/09830 A1



— Vor Ablauf der für Änderungen der Ansprüche geltenden Frist: Veröffentlichung wird wiederholt, falls Änderungen eintreffen.

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

WO 01/09830 .

PCT/DE00/02606

5

Verfahren zur Archivierung digital signierter Dokumente auf Papier und ähnlichen Materialien

10

Die Erfindung betrifft ein Verfahren zur Archivierung digital signierter Dokumente auf Papier und ähnlichen Materialien. Mit seiner Hilfe lassen sich die Vorteile digitaler signierter Dokumente mit den Vorteilen von Dokumenten in Papierform verbinden. Digital signierte Dokumente zeichnen sich insbesondere dadurch aus, daß sie auf elektronischem Weg versandt werden können. Es entfällt daher der heutzutage notwendige physische Transport materieller Beweisgegenstände. Digital signierte Dokumente gelten zudem als hochgradig fälschungssicher. Für Dokumente in Papierform spricht in vielen Anwendungsbereichen der einfache Zugriff auf die enthaltenen Informationen ohne technische Hilfsmittel sowie die Möglichkeit zur sicheren und zuverlässigen Aufbewahrung.

15

20

Stand der Technik

25

Electronic Commerce entwickelt sich zu einem zunehmend bedeutenderen Wirtschaftsfaktor. Im Idealfall geschieht ein Geschäftsabschluß und - sofern die Natur des Geschäfts keinen Austausch materieller Güter erfordert - die Leistungserbringung allein durch den Austausch elektronischer Dokumente, d.h. digitaler Daten. Auf den Versand konventioneller Dokumente in Papierform, z.B. Angebotsschreiben, wird dabei verzichtet. Dadurch ergeben sich zahlreiche Vorteile. So ist die Übermittlung digitaler Daten üblicherweise wesentlich schneller und kostengünstiger als der Versand konventioneller Dokumente. Falls die Computersysteme beider Transaktionspartner

30

WO 01/09830

PCT/DE00/02606

2

sinnvoll aufeinander abgestimmt sind, können die Transaktionen zudem automatisiert bearbeitet werden, wodurch sich erhebliche Rationalisierungseffekte ergeben.

5 Allerdings birgt der Verzicht auf konventionelle Dokumente auch Nachteile, insbesondere hinsichtlich der Beweislage. Werden keine besonderen Vorkehrungen getroffen, lassen sich digitale Daten relativ leicht fälschen, ohne daß es im Nach-
10 hinein erkennbar ist. Unter diesen Voraussetzungen ist der Beweiswert der im Zuge elektronischer Transaktionen übermittelten elektronischen Dokumente relativ gering. Die Beweislage bei elektronischen Transaktionen ist daher im allgemeinen unbefriedigend.

15 Digitale Signaturverfahren bieten eine Lösung für dieses Problem. Sie basieren auf asymmetrischen Verschlüsselungsverfahren, die auch als Public-Key-Verfahren bezeichnet werden (vgl. z.B. W. Diffie und M.E. Hellman, "New directions in cryptography", in IEEE Transactions on Information Theory, Vol. IT-22, November 1976, Seiten 644-654; sowie R. Rivest,
20 A. Shamir und L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", in Communications of the ACM, Vol. 27, Nr. 2; Februar 1978, Seiten 120-126). Dabei wird jeder Person, die elektronische Dokumente digital
25 signieren will, ein Paar korrespondierender Schlüssel zugeordnet. Der erste Schlüssel wird zum Erzeugen einer Signatur verwendet und ist nur dem jeweiligen Inhaber bekannt. Der zweite Schlüssel dient zum Überprüfen einer mit dem ersten Schlüssel generierten Signatur und wird unter der Angabe des
30 Inhabers des Schlüsselpaars öffentlich bekanntgemacht.

Das Signieren eines elektronischen Dokuments geschieht, indem es mit dem geheimen Schlüssel des Unterzeichners verschlüsselt wird. Mit Hilfe des öffentlichen Schlüssels des Unter-

zeichners kann jedermann das Dokument wieder entschlüsseln, d.h. die Signatur überprüfen. Nur wenn der zum Entschlüsseln benutzte öffentliche Schlüssel mit dem zum Verschlüsseln benutzten geheimen Schlüssel korrespondiert, resultiert aus dem Entschlüsselungsvorgang das ursprüngliche Dokument. Wurde das Dokument nach dem Signieren verändert oder wird der falsche öffentliche Schlüssel zum Entschlüsseln benutzt, resultiert eine scheinbar zufällige Folge von Daten ohne erkennbaren Sinn. Da nur der Inhaber des geheimen Schlüssels ein Dokument derart verschlüsseln kann, daß es sich mit dem korrespondierenden öffentlichen Schlüssel wieder sinnvoll entschlüsseln läßt, muß er sich den Inhalt eines erfolgreich mit seinem öffentlichen Schlüssel entschlüsselten Dokuments zurechnen lassen.

Mit digitalen Signaturverfahren besteht demnach die Möglichkeit, immaterielle Beweisstücke zu generieren. Diverse Verfahren und Protokolle, die auf dem grundsätzlichen Konzept der digitalen Signatur aufbauen, sind z.B. in dem Buch „Applied Cryptography - Protocols, Algorithms, and Source Code in C“ (Bruce Schneier, 2. Auflage 1996, New York, Chichester u.a.) beschrieben. Sofern digitale Signaturverfahren auf breiter Basis angewendet werden und digital signierte Dokumenten in der Rechtsprechung ein ähnlich hoher Beweiswert wie konventionellen Dokumenten aus Papier eingeräumt wird, läßt sich trotz Verzichts auf konventionelle Dokumente eine hohe Rechtssicherheit im Electronic Commerce erreichen. Digital signierte Dokumente weisen jedoch unter anderem die folgenden Probleme auf:

a) Handhabungsproblem

Zur Darstellung digital signierter Dokumente sind technische Hilfsmittel, z.B. Personalcomputer, unabdingbar. In Berei-

chen, in denen entsprechende Systeme ständig bereitstehen, z.B. im Bürobereich, bereitet dieses keine Probleme. Vor allem bei Privatanwendern sind jedoch Personalcomputer oder ähnliche Systeme, sofern sie überhaupt zur Verfügung stehen, nicht immer im betriebsbereiten Zustand. In solchen Fällen ist das Einsehen von Informationen auf einem Dokument aus Papier schneller und unkomplizierter als das Einsehen der entsprechenden Informationen in einem digital signierten Dokument.

b) Aufbewahrungsproblem

Ein großes Problem stellt die sichere Aufbewahrung digital signierter Dokumente dar. Diese unterscheiden sich technisch in keiner Weise von anderen digitalen Daten und sind deshalb denselben Gefahren ausgesetzt. Durch Computerviren, unbeabsichtigtes Löschen von Dateien, einen Festplatten-Defekt oder ähnliche unerwünschte Vorkommnisse können wichtige Beweismstücke unwiderruflich verloren gehen. Aus diesem Grund müssen Sicherheitskopien dieser Unterlagen angefertigt werden. In der Praxis werden jedoch Sicherheitskopien aufgrund des damit verbundenen Aufwands meist nur sporadisch angefertigt. Zudem handelt es sich bei den eingesetzten Geräten oftmals um Systeme, die nicht immer zuverlässig funktionieren bzw. bei denen die Langzeitbeständigkeit der archivierten Daten nicht gewährleistet ist, z.B. CD-ROM-Brenner oder Schreib-/Lesegeräte für magnetische Wechselmedien. Darüber hinaus ist nicht bei allen Systemen sichergestellt, daß nach einem Zeitraum von mehreren Jahren noch Lesegeräte für die entsprechenden Medien hergestellt werden. Wenn in einem solchen Fall das eingesetzte Lesegerät nicht mehr funktioniert und sich kein Ersatz dafür besorgen läßt, sind die archivierten Daten wertlos. Dokumente aus Papier können hingegen problemlos über

Jahrzehnte hinweg aufbewahrt und ohne technische Hilfsmittel gelesen werden.

5 In vielen Anwendungsbereichen ist daher die Aufbewahrung von Dokumenten in Papierform vorteilhaft gegenüber der Aufbewahrung in digitaler Form. Um dennoch die Vorteile des Electronic Commerce nutzen und auf den physischen Transport konventioneller Dokumente verzichten zu können, bietet es sich an, Papier als Datenträger für digital signierte Daten zu verwenden.
10

15 Damit die digitale Signatur bei dieser Form der Aufbewahrung ihren Sinn behält, müssen sowohl die signierten Daten als auch die Signatur derart auf dem Papier abgelegt sein, daß die ursprünglichen digitalen Daten sich bitgetreu anhand des Papiers rekonstruieren lassen. Dieses ist deshalb notwendig, weil bereits die Änderung eines einzigen Bits am signierten Dokument zur Ungültigkeit der digitalen Signatur führt. Zur bitgetreuen Ablage digitaler Daten auf Papier stehen mehrere
20 Verfahren zur Verfügung. Die einfachste Möglichkeit besteht darin, alphanumerische Zeichen auf das Papier zu drucken. Diese können bei Bedarf manuell in ein Computersystem eingegeben oder durch optische Texterkennung (OCR) eingelesen werden. Sofern eindeutig geregelt ist, wie diese Zeichen zu interpretieren sind, lassen sich dadurch die ursprünglichen digitalen Daten rekonstruieren.
25

30 US-Patent 5.214.702 beschreibt eine Variante, bei der aus einem digitalen Textdokument auf genau definierte Weise jegliche Zeichen entfernt werden, die in einem Ausdruck überhaupt nicht bzw. nicht eindeutig zu erkennen sind, z.B. Tabulatorzeichen, mehrfache Leerzeichen oder Zeilenumbrüche. Das resultierende Textdokument wird digital signiert. Danach kann das ursprüngliche Textdokument zusammen mit der digitalen Si-

WO 01/09830 .

PCT/DE00/02606

6

gnatur ausgedruckt werden. Um zu einem späteren Zeitpunkt die Signatur zu überprüfen, werden der auf dem Papier stehende Text und die digitale Signatur in ein Computersystem eingegeben. Aus dem eingegebenen Text werden auf dieselbe Art wie
5 beim ursprünglichen Textdokument alle Tabulatorzeichen, mehrfache Leerzeichen, Zeilenumbrüche etc. entfernt, so daß genau dasselbe Textdokument resultiert, das vor Anfertigung des Ausdrucks digital signiert wurde. Anhand des resultierenden Textdokuments kann die digitale Signatur überprüft werden.
10 Mit Hilfe des Verfahrens können z.B. E-Mails vor dem Versand digital signiert werden. Der Empfänger der E-Mail kann sie zusammen mit der digitalen Signatur ausdrucken und den Ausdruck sicher aufbewahren. Anhand des Ausdrucks kann jederzeit die digitale Signatur überprüft werden, ohne daß auf die ursprünglich empfangene, in digitaler Form vorliegende E-Mail
15 zurückgegriffen werden muß.

Das Verfahren eignet sich somit, einen großen Teil der digital signierten Dokumente, die im Rahmen elektronischer Transaktionen ausgetauscht werden, in Papierform zu archivieren.
20 Nachteilig ist bei diesem Verfahren, daß nur sehr einfach strukturierter Text digital signiert werden kann. Textdokumente, die Formatierungen (z.B. Unterstreichungen oder Fettschrift), komplexe Textanordnungen (z.B. mehrspaltigen Text) oder graphische Elemente enthalten, können mit Hilfe des Verfahrens nicht digital signiert werden. Theoretisch kann das Verfahren derart erweitert werden, daß solche Textdokumente
25 auch digital signiert werden können; die Komplexität des Verfahrens steigt dabei jedoch um ein Vielfaches. Ein weiterer Nachteil ist die Beschränkung auf einen bestimmten Zeichenvorrat. Zeichen, die nicht im Verfahren vorgesehen sind, z.B. das neue Euro-Symbol, können nicht verwendet werden, solange
30 das Verfahren nicht entsprechend erweitert wird.

Eine weitere Möglichkeit, Daten bitgetreu auf Papier abzulegen, besteht in der Verwendung sogenannter Barcodes. Hierbei werden digitale Daten auf genau definierte Weise in eine lineare Folge weißer und schwarzer Rechtecke transformiert. Dieses Muster kann mit einem handelsüblichen Drucker auf Papier ausgegeben werden. Um die ursprünglichen digitalen Daten zu rekonstruieren, wird das Muster mit einem sogenannten Barcode-Scanner optisch abgetastet. Daraus resultiert ein elektronisches Abbild des Musters, aus dem mit Hilfe elektronischer Bildverarbeitungsverfahren die ursprünglichen digitalen Daten rekonstruiert werden können. Der Einsatz dieser Verfahren ist weitverbreitet. So findet sich z.B. auf den Verpackungen der meisten Lebensmittel und Konsumgüter ein Barcode-Muster, das mit Hilfe entsprechender Kassensysteme genutzt werden kann.

Eine Erweiterung dieser Verfahren sind sogenannte zweidimensionale Barcodes, die z.B. in den US-Patenten 5.504.322 und 5.862.270 beschrieben sind. Diese kann man sich vorstellen als eine Vielzahl herkömmlicher Barcode-Muster gleicher Länge, die ohne Zwischenraum untereinander angeordnet werden. Die einzelnen Barcode-Muster werden dabei gestaucht. Während bei herkömmlichen Barcode-Mustern die einzelnen Rechtecke meist die Form länglicher vertikaler Striche haben, ist ihre Form bei zweidimensionalen Barcode-Mustern im allgemeinen quadratisch. Der Vorteil zweidimensionaler Barcodes liegt in der größeren Datenmenge, die auf einer gegebenen Fläche untergebracht werden kann. Allerdings sind aufwendigere Geräte zur optischen Abtastung notwendig, da ein zweidimensionales Muster erfaßt werden muß. Zudem müssen komplexere Bildverarbeitungsverfahren zum Einsatz kommen, um aus dem elektronischen Abbild des Musters die ursprünglichen digitalen Daten zu rekonstruieren.

WO 01/09830 .

PCT/DE00/02606

8

Da mit Barcodes beliebige digitale Daten eindeutig auf Papier abgelegt werden können, eignen sich diese Verfahren prinzipiell auch für beliebige digital signierte Daten. Ein Anwendungsbeispiel ist die elektronische Frankierung von Poststücken, bei der unter anderem die Adreßdaten des Empfängers sowie eine eindeutige Seriennummer digital signiert und in Form eines zweidimensionalen Barcodes mittels eines handelsüblichen Druckers auf einen normalen Briefumschlag ausgedruckt werden (vgl. United States Postal Service, Information-based indicia program (IBIP) - Performance criteria for information-based indicia and security architecture for open IBI postage evidencing systems (PCIBI-O), Entwurf vom 25.06.1999, Seite A-3; erhältlich unter <http://www.usps.gov/ibip/documents/specs/pcibi-625.pdf>).

Mit Hilfe von Barcode-Verfahren können demnach sämtliche Daten, die bei elektronischen Transaktionen anfallen, in Papierform archiviert werden. Von großem Nachteil ist dabei allerdings, daß die Barcode-Muster nicht direkt für Menschen lesbar sind.

Ein weiteres Verfahren, um digitale Signaturen in Verbindung mit Papier oder ähnlichen Materialien zu verwenden, ist in WO 94/19770 beschrieben. Gegenstand dieser Veröffentlichung ist ein sicheres Personenidentifizierungsinstrument. Sowohl die Textdaten als auch das Foto des Inhabers sind bei dieser Erfindung durch die digitale Signatur der ausstellenden Behörde vor Fälschungen geschützt. Das Foto wird dabei für den Signiervorgang auf eine eindeutig zu reproduzierende Bitfolge reduziert, indem mehrere globale Merkmale des Bildes extrahiert und in kleinen Zahlen kodiert werden. Die jeweils resultierenden Bitfolgen lassen sich zu einer einzelnen Bitfolge zusammenfassen. Der gleiche Vorgang wird bei der Überprüfung der digitalen Signatur ausgeführt.

Während sich dieses Verfahren für den Bereich der Personen-identifizierungsinstrumente eignet, ist es allerdings nur für einen Bruchteil der Dokumente einzusetzen, die im Rahmen elektronischer Transaktionen ausgetauscht werden. Damit aus dem Ausdruck eines Fotos auf Papier die gleichen Merkmalswerte wie aus dem ursprünglichen Foto extrahiert werden können, sind zudem hohe Anforderungen an das verwendete Druckverfahren zu stellen.

Aufgabe

Die genannten Verfahren eignen sich nur bedingt dazu, die im Rahmen elektronischer Transaktionen ausgetauschten digital signierten Dokumente in Papierform zu archivieren. Der Erfindung liegt daher die Aufgabe zugrunde, digital signierte Dokumente zu erzeugen, die möglichst wenigen Beschränkungen hinsichtlich ihres Inhalts oder ihrer graphischen Gestaltung unterliegen und die direkt für Menschen lesbar sind, sowie diese mittels eines handelsüblichen Computersystems in Verbindung mit einem handelsüblichen Drucker auf Papier oder ähnlichen Materialien auszugeben.

Damit ein derartig erzeugter Ausdruck eines digital signierten Dokuments archiviert werden und später als Beweisgegenstand dienen kann, liegt der Erfindung außerdem die Aufgabe zugrunde, die digitale Signatur des Ausdrucks auf einfache Art und Weise zu überprüfen, ohne daß ein Rückgriff auf das ursprünglich im Computersystem vorliegende Dokument nötig ist.

Sowohl bei der Erzeugung als auch bei der Überprüfung eines Dokuments sollen dabei die Anforderungen des deutschen Signaturgesetzes, der europäischen Signaturrechtlinie oder anderer Regelwerke im Bezug auf digitale Signaturen berücksichtigt werden können.

WO 01/09830

PCT/DE00/02606

10

Diese Aufgabe wird erfindungsgemäß durch ein Verfahren zur Darstellung digital signierter elektronischer Dokumente in gedruckter Form und zur Verifikation der Signatur aus der gedruckten Form gelöst, bei dem zur Darstellung des Dokuments in gedruckter Form das elektronische Dokument in Form einer zweidimensionalen Matrix von Bildpunkten (Bitmap) dargestellt wird, Daten der zweidimensionalen Matrix von Bildpunkten (Bitmap) mittels des geheimen Schlüssels der digitalen Signatur verschlüsselt werden und die verschlüsselten Daten und die Bitmap in zumindest auch maschinenlesbarer Form gedruckt werden und zur Verifikation der Signatur die gedruckte Form gescannt wird, aus dem durch das Scannen gewonnenen digitalen Abbild die zweidimensionale Matrix von Bildpunkten (Bitmap) und die digitale Signatur rekonstruiert wird und die rekonstruierte Signatur anhand der rekonstruierten Matrix von Bildpunkten (Bitmap) verifiziert wird.

Vorzugsweise kann die Bitmap dabei gleichzeitig einen für Menschen lesbaren Ausdruck des digital signierten Dokuments darstellen und gleichzeitig maschinenlesbar sein. Auf diese Weise ist eine vollautomatische Kontrolle der Echtheit des Dokuments möglich. Dabei ist jedoch ein sehr genaues Einscannen des Bitmap erforderlich.

Um die Zahl der einzuscannenden Daten zu vermindern und das Scannen zu vereinfachen, ist es daher besonders bevorzugt, das digital signierte Dokument parallel in für Menschen lesbarer und maschinenlesbarer Form auszudrucken und bei der Verifikation der Signatur die maschinenlesbare Form einzuscannen und damit die ursprünglichen Daten zu rekonstruieren und die Daten der Bitmap aus den ursprünglichen Daten wieder herzustellen und sodann die Daten der wiederhergestellten Bitmap

WO 01/09830

PCT/DE00/02606

11

mit dem in für Menschen lesbarer Form ausgedruckten Dokument zu vergleichen.

5 Vorzugsweise kann dieser Vergleich automatisch mittels spezieller Bildverarbeitungsverfahren erfolgen, die signifikante Abweichungen anzeigen. Auf diese Weise ist auch hier ein zumindest "halbautomatischer" Vergleich möglich.

10 Um die Zahl der zu handhabenden Daten weiter zu reduzieren, ist es besonders bevorzugt, daß die Daten der Bitmap vor der Verschlüsselung komprimiert und vor der Verifikation dekomprimiert werden.

15 Der Ausdruck in maschinenlesbarer Form erfolgt vorzugsweise als zweidimensionaler Barcode. Dadurch läßt sich ein Maximum an Datendichte erreichen.

20 Weiter ist es zur Verifikation bevorzugt, daß der für den Menschen lesbare Ausdruck des Bitmaps mit einem Rahmen mit in regelmäßigem Abstand angeordneten Markierungen umgeben ist.

25 Bei jedem Ausdruck eines elektronischen Dokuments wird eine Bitmap erzeugt, entweder bereits im Computer oder spätestens im Drucker. Im Gegensatz zu diesem Normalfall wird im beschriebenen Verfahren eine Bitmap im Computer erzeugt, die jedoch nicht direkt an einen Drucker weitergeleitet sondern für die weiteren Verfahrensschritte im Computer gespeichert wird. In der Mehrzahl der Fälle wird eine Monochrom-Bitmap ausreichen, die nur die beiden Farbabstufungen Schwarz und
30 Weiß enthält. Graustufen-Bitmaps oder Farb-Bitmaps sind grundsätzlich auch möglich, allerdings ist bei diesen Arten besonders darauf zu achten, daß die Größe der Bitmap nach dem Komprimieren bestimmte Grenzen nicht überschreitet (siehe unten). Unabhängig davon sollte bei der Erzeugung der Bitmap

ein weitverbreitetes Format wie z.B. das Windows Bitmap-Format oder das unkomprimierte TIF-Format gewählt werden. Dadurch wird die weitere Verarbeitung der Bitmap durch gegebenenfalls eingesetzte externe Programme bzw. Programmbibliotheken erleichtert.

Das Signieren der Bitmap kann auf verschiedene Arten erfolgen. Sofern das Dokument von einem menschlichen Benutzer signiert wird, ist der Einsatz einer Chipkarte in Verbindung mit einem Chipkartenleser zu empfehlen, um den Anforderungen des Signaturgesetzes zu entsprechen. In diesem Fall ist die Bitmap zunächst dem Unterzeichner anzuzeigen und eine Bestätigung für den Signiervorgang anzufordern. Sofern der Unterzeichner die Bestätigung erteilt, ist im Computer der Hash-Wert der Bitmap zu berechnen und an die Chipkarte zu übergeben. Dieser wird innerhalb der Chipkarte mittels des dort gespeicherten geheimen Schlüssels des Unterzeichners und des hardwaremäßig implementierten Signaturalgorithmus verschlüsselt. Das Ergebnis des Verschlüsselungsvorgangs ist die digitale Signatur, die zur weiteren Verarbeitung von der Chipkarte an den Computer übergeben wird.

Bei einer automatisierten Generierung von Dokumenten, z.B. auf einem Web-Server, kann auf die Anforderung einer manuellen Bestätigung durch einen menschlichen Benutzer verzichtet werden. Auch auf den Einsatz von Chipkarten kann verzichtet und die entsprechenden Routinen können zusammen mit dem geheimen Schlüssel des Servers in Software implementiert werden, sofern ein Zugriff durch Unbefugte durch technische und organisatorische Maßnahmen ausgeschlossen wird.

Unabhängig von einer manuellen oder automatisierten Erzeugung der Signatur sollten dabei die gesetzlich zugelassenen Algorithmen verwendet werden, um die spätere Anerkennung vor Ge-

richt nicht zu gefährden. In Übereinstimmung mit den Anforderungen des Signaturgesetzes werden z.B. häufig RIPEMD-160 als Hash-Verfahren und RSA als Verschlüsselungsverfahren verwendet (vgl. Bundesanzeiger Nr. 213 Seite 18.638, vom 11. November 1999, erhältlich unter

http://www.rectp.de/imperia/md/content/tech_reg_t/digisign/9.pdf).

Für die spätere Archivierung in digitaler Form auf einem Ausdruck ist die Speicherbedarf einer unkomprimierten Bitmap mit akzeptabler Auflösung zu groß. Daher ist eine Komprimierung der Bitmap sinnvoll. Für schwarzweiße Textdokumente mit lediglich geringem Anteil graphischer Elemente stehen hocheffiziente Komprimierungsalgorithmen zur Verfügung. Hierbei ist vorrangig der zukünftige JBIG2 Standard der Joint Bi-level Image Experts Group zu nennen (vgl. JBIG2 working draft, erhältlich unter <http://www.jbig.org/public/wd14492.pdf>). Auch für Graustufenbilder und Farbbilder wurden in den letzten Jahren große Fortschritte bezüglich der erzielbaren Komprimierungsraten bei akzeptabler Darstellungsqualität erzielt. Experimente mit verschiedenen einseitigen Dokumenten im DIN A4-Format, die einen repräsentativen Querschnitt in der Praxis vorkommender Geschäftsbriefe und anderer Dokumente bezüglich graphischer Gestaltung und Textumfang darstellen, haben ergeben, daß sich eine daraus abgeleitete Bitmap mit 300 dpi Auflösung fast immer mit weniger als 20 kByte und sehr häufig sogar mit weniger als 10 kByte kodieren läßt. Durch Weglassen graphischer Elemente, das Vermeiden unterschiedlicher Textgrößen und Schriftformen sowie eine Reduzierung auf 200 dpi läßt sich dieser Speicherbedarf nochmals deutlich reduzieren, was z.B. bedeutsam sein kann, wenn Tintenstrahldrucker oder Faxgeräte als Ausgabegeräte genutzt werden sollen (siehe unten).

Die Komprimierung der Bitmap sollte in verlustfreier Form geschehen, d.h. aus der komprimierten Form muß sich die ursprüngliche digital signierte Bitmap bitgetreu rekonstruieren lassen. Das bedeutet jedoch nicht, daß auf den Einsatz von Komprimierungsalgorithmen verzichtet werden muß, die einen Großteil ihrer Effizienz durch das Weglassen von für das menschliche Auge kaum wahrnehmbaren Bilddetails erzielen. Will man derartige Verfahren verwenden, müssen jedoch diejenigen Verfahrensschritte, bei denen unauffällige Bilddetails entfernt werden, vor dem Signieren ausgeführt werden. Nach dem Signieren dürfen nur noch verlustfreie Komprimierungsschritte vorgenommen werden. Dadurch wird einerseits dem Unterzeichner genau die Bitmap angezeigt, die er letzten Endes signiert, und andererseits ist die bitgetreue Rekonstruktion der signierten Bitmap möglich.

Statt einer komprimierten Bitmap kann auch ein aus dem ursprünglichen elektronischen Dokument abgeleitetes Zwischenformat archiviert werden, z.B. Postscript- oder HTML-Code, aus dem sich in eindeutiger Weise die ursprünglich digital signierte Bitmap rekonstruieren läßt. Bei dieser Variante ist man zwar weniger flexibel als bei der Verwendung einer komprimierten Bitmap, dafür kann unter bestimmten Bedingungen der Speicherplatzbedarf gegenüber einer komprimierten Bitmap erheblich reduziert werden. Wie bereits erwähnt, kann dieser Umstand bedeutsam bei der Verwendung von Tintenstrahldruckern oder Faxgeräten sein (siehe unten). Um die durch Verwendung des Bitmap-Formats erreichte Flexibilität nicht einzubüßen, sollten Varianten wie die Archivierung von HTML- oder Postscript-Code zusätzlich zu einer stets verfügbaren Archivierung in Form komprimierter Bitmaps angeboten werden.

Variationen des Verfahrens sind auch möglich bezüglich der Frage, ob die unkomprimierte Bitmap, die komprimierte Bitmap oder ein gegebenenfalls verwendetes Zwischenformat digital signiert werden soll. Das Signieren der unkomprimierten Bitmap erscheint die sinnvollste Variante, da somit diejenige Softwarekomponente, welche für die Anzeige der signierten bzw. zu signierenden Daten verwendet wird, die geringstmögliche Komplexität und Fehleranfälligkeit aufweist. Diese Tatsache ist unter anderem deshalb von Bedeutung, da diese Softwarekomponente nach dem deutschen Signaturgesetz einer aufwendigen Sicherheitsüberprüfung unterliegt, sofern die Software offiziell zertifiziert werden soll.

Die komprimierte Bitmap und die digitale Signatur bilden die wesentlichen zu archivierenden Daten. In den meisten Fällen wird es jedoch sinnvoll sein, diese Daten um das Zertifikat des Unterzeichners zu ergänzen. Bei einem Zertifikat handelt es sich um eine von einer Zertifizierungsstelle digital signierte Datei, die persönliche Angaben des Unterzeichners (unter anderem Name und Anschrift), dessen öffentlichen Schlüssel sowie Angaben zu den verwendeten kryptographischen Verfahren enthält. Die Zertifizierungsstelle ist eine vertrauenswürdige Instanz, auf deren Angaben sich die Benutzer digitaler Signaturverfahren verlassen können. Aus dem Zertifikat läßt sich demnach in beglaubigter Form ermitteln, wer das Dokument unterzeichnet hat und welcher öffentliche Schlüssel beim Überprüfen der Signatur zu verwenden ist. Signatur und Zertifikat haben einen Speicherbedarf von zusammen ca. einem kByte.

Eine Ergänzung der Bitmap, der digitalen Signatur und gegebenenfalls des Zertifikats um weitere Daten kann sinnvoll sein, wenn eine automatisierte Verarbeitung auf dem Computersystem des Empfängers gewünscht wird. Hierbei ist jedoch sicherzu-

WO 01/09830

PCT/DE00/02606

16

stellen, entweder durch manuelle Überprüfung durch den Empfänger bzw. durch automatisierte Plausibilitätskontrollen, daß diese zusätzlichen Daten nicht den Angaben in der digital signierten Bitmap widersprechen.

5

10

15

Aus den zu archivierenden Daten wird danach ein zweidimensionaler Barcode erzeugt. Hierfür steht z.B. das Produkt „Paperdisk“ der US-amerikanischen Firma Cobblestone Software, Inc. zur Verfügung, welches sich in den bisherigen Tests durch hohe erzielbare Datendichten bei gleichzeitig hoher Zuverlässigkeit auszeichnete (vgl. z.B. T. Antognini und W. Antognini, „A flexibly configurable 2D bar code“, Papier präsentiert auf dem Information Based Indicia Program Technology Symposium des United States Postal Service, 25.-26. November, 1996, erhältlich unter <http://www.paperdisk.com/ibippapr.htm>). Der Einsatz anderer zweidimensionaler Barcodeverfahren ist ebenso denkbar.

20

25

30

Bei der Erzeugung des Barcodes muß ein Kompromiß eingegangen werden zwischen hoher Datendichte und zuverlässiger Rekonstruktion der im Barcode enthaltenen digitalen Daten. Durch die Verwendung von Fehlerkorrekturverfahren läßt sich die Zuverlässigkeit des Verfahrens wesentlich steigern. Das bereits genannte „Paperdisk“-Verfahren verwendet ein Reed-Solomon-Korrekturverfahren mit frei wählbarer Redundanz. Wenn man Laserdrucker mit 600 dpi Auflösung verwendet, kann damit bei 29% Redundanz eine effektive Datendichte von ca. 500 Byte Nutzdaten pro cm² erzielt werden. Bei Tintenstrahldruckern sollte die effektive Datendichte auf ca. 270 Byte/cm² und bei Faxgeräten auf ca. 130 Byte/cm² reduziert werden. Geht man von einem Barcode mit einer maximalen Breite von 18 cm und einer maximalen Höhe von 2 cm aus, was sich als praktikable Größenbeschränkung erwiesen hat, können somit maximal 18 kByte, 9,7 kByte bzw. 4,7 kByte Nutzdaten auf einem Ausdruck

untergebracht werden. Zieht man davon 1 kByte für die digitale Signatur und das Zertifikat ab, darf die komprimierte Bitmap maximal 17 kByte, 8,7 kByte bzw. 3,7 kByte groß sein.

5 Die ursprüngliche Bitmap und der Barcode können zu einem elektronischen Dokument zusammengefaßt werden. Um den durch die digitale Signatur geschützten Bereich zu verdeutlichen, bietet es sich an, die Bitmap deutlich sichtbar durch einen Rahmen zu begrenzen. Da sowohl beim Ausdruck als auch beim
10 späteren Einscannen des Dokuments geometrische Verzerrungen auftreten können, bietet es sich zusätzlich an, in regelmäßigen Abständen kleine Markierungen am Rahmen zu platzieren, mit deren Hilfe beim späteren Vergleich zwischen der sichtbaren Bitmap und der im Barcode in digitaler Form enthaltenen Bit-
15 map eine Verzerrungskorrektur vorgenommen werden kann. Als Format für das zu erzeugende elektronische Dokument bietet sich z.B. das „Portable Document Format“ (PDF) der US-amerikanischen Firma Adobe Systems Incorporated an, da es auf einem großen Anteil aller im Einsatz befindlichen Computer
20 installiert ist (vgl. „Portable Document Format Reference Manual Version 1.3“, erhältlich unter <http://partners.adobe.com/asn/developer/acrosdk/DOCS/pdftspec.pdf>). Bei Verwendung dieses Formats kann ein Empfänger mit hoher Wahrscheinlichkeit einen Ausdruck des Dokuments erzeugen, ohne sich extra zu diesem Zweck zusätzliche Software zu
25 besorgen.

Wenn vorausgesetzt wird, daß der Empfänger über entsprechende Software verfügt bzw. sie sich besorgen kann, ist auch die
30 Verwendung eines wesentlich kompakteren Formats möglich. Diese Variante ist besonders bei Übertragungswegen mit geringer Bandbreite und bei häufigem Austausch verfahrensmäßig erzeugter Dokumente empfehlenswert. Zusätzlich ergibt sich beim Einsatz entsprechender Software für den Empfänger die Mög-

lichkeit, die digitale Signatur des Dokuments bereits vor dem Ausdruck zu überprüfen.

Das erzeugte Dokument kann auf verschiedene Arten an den Empfänger übermittelt werden. Wenn das Dokument manuell erzeugt wurde, kann der Unterzeichner es z.B. per E-Mail-Anhang an den Empfänger senden. Bei Web-basierten Systemen, bei denen das Dokument auf der Grundlage eines interaktiven Dialogs mit dem Empfänger automatisiert generiert wird, kann die Übertragung des Dokuments auch per „Hypertext Transfer Protocol“ (HTTP) erfolgen.

Nach der Anfertigung eines Ausdruck empfiehlt es sich, die digitale Signatur des Ausdrucks sofort zu überprüfen. Dadurch wird sichergestellt, daß Fehler im Ausdruck oder Verunreinigungen des Papiers nicht die Bestätigung der digitalen Signatur verhindern. Erst danach sollte das Dokument sicher verwahrt werden. Gelingt die Bestätigung der digitalen Signatur nicht, sollte ein neuer Ausdruck angefertigt werden. Die Entscheidung, ob eine sofortige Überprüfung vorgenommen wird, liegt im Ermessen des Benutzers und wird sich an der Wichtigkeit des Dokuments orientieren.

Falls ein elektronisches Dokument sich nicht sinnvoll auf einer einzigen Seite darstellen läßt, können mit Hilfe des erfindungsgemäßen Verfahrens auch mehrseitige Dokumente in Papierform erzeugt werden. Hierzu stehen verschiedene Optionen zur Verfügung. Eine Option, die weitgehend dem Verhalten anderer digitaler Signaturverfahren entspricht, besteht darin, die für jede einzelne Seite des Dokuments erzeugten Bitmaps in einem einzigen Dokument zusammenzufassen und dieses Dokument zu signieren. Anschließend können die Bitmaps für jede Seite einzeln auf die beschriebene Weise verarbeitet werden, wobei die digitale Signatur und das Zertifikat nur auf einer

der Seiten archiviert werden müssen. Entsprechend sind beim Überprüfen des Dokuments nach dem Einscannen aller Seiten des Dokuments zunächst alle einzelnen Bitmaps zu einem einzigen Dokument zusammenzufassen, anhand dessen die Signatur überprüft werden kann. Da bei Dokumenten mit vielen Seiten das Einscannen jeder einzelnen Seite sehr lästig sein kann, bietet sich im Anschluß an den Ausdruck des Dokuments der zusätzliche Ausdruck einer Seite an, auf der in zusammengefaßter Form alle zweidimensionalen Barcodes der einzelnen Seiten enthalten sind. In diesem Fall genügt das Einscannen dieser einen Seite, wobei allerdings auf den unten beschriebenen Vergleich zwischen den sichtbaren Bitmaps und den im Barcode enthaltenen Bitmaps verzichtet werden muß.

Bei der optischen Abtastung sollte eine Auflösung von mindestens 300 dpi verwendet werden, damit für die anschließende elektronische Bildverarbeitung zur Rekonstruktion der in dem Barcode enthaltenen digitalen Daten möglichst viele Informationen zur Verfügung stehen. Aus demselben Grund empfiehlt sich, bei der optischen Abtastung Graustufen zu erfassen. Bei schlechter Qualität des Ausdrucks kann auch die Verwendung einer Auflösung von 400 dpi oder 600 dpi notwendig sein.

Sofern die Decodierung des eingescannten Barcodes gelingt, kann anhand der darin enthaltenen Daten die Signatur überprüft werden. Wie bereits erwähnt, wird der Barcode neben der komprimierten Bitmap und der digitalen Signatur im allgemeinen das Zertifikat des Unterzeichners enthalten. Aus diesem können der zum Überprüfen zu verwendende öffentliche Schlüssel des Unterzeichners sowie die zum Überprüfen einzusetzenden Verfahren abgeleitet werden. Sofern kein Zertifikat enthalten ist, muß dieses in der lokalen Datenbank bzw. bei der Zertifizierungsstelle, die das Zertifikat ursprünglich ausgestellt hatte, abgefragt werden. Da dieser Vorgang nach eini-

gen Jahren sehr mühsam, wenn nicht gar unmöglich sein kann, empfiehlt sich das Weglassen des Zertifikats für langfristig zu archivierende Dokumente nicht. Oftmals ist auch bei enthaltenem Zertifikat eine Anfrage bei der zuständigen Zertifizierungsstelle sinnvoll, um zu überprüfen, ob das Zertifikat nicht bereits zum vorgeblichen Unterzeichnungszeitpunkt gesperrt war.

Für den weiteren Verlauf der Signaturprüfung wird die komprimierte Bitmap dekomprimiert und auf gleiche Weise wie beim Erzeugen des Dokuments der Hash-Wert der dekomprimierten Bitmap erzeugt. Dieser wird anschließend mit dem Wert verglichen, der sich durch das Entschlüsseln der digitalen Signatur mit dem öffentlichen Schlüssel des Unterzeichners ergibt. Stimmen beide Werte überein, ist die Signaturprüfung erfolgreich, und die dekomprimierte Bitmap wird dem Überprüfenden zusammen mit einer entsprechenden Meldung auf dem Bildschirm angezeigt. Der Überprüfende hat in diesem Fall die Gewähr, daß der vorgebliche Unterzeichner tatsächlich eine Willenserklärung abgegeben hat, die sich mit der auf dem Bildschirm angezeigten Willenserklärung deckt.

Die Anzeige auf dem Bildschirm gibt die digital signierte Willenserklärung wieder und stellt somit ein gerichtsverwertbares Beweisstück dar. Die auf dem Ausdruck enthaltene, mit bloßem Auge erkennbare Bitmap hingegen kann ohne weiteres verändert werden, ohne daß das Ergebnis der beschriebenen Signaturprüfung verändert wird. Sie ist somit vom Gesichtspunkt der Beweisführung her überflüssig. Theoretisch würde zu diesem Zweck die alleinige Archivierung des ausgedruckten Barcodes genügen. Aus Sicht des Benutzers hat die im Ausdruck mit bloßem Auge erkennbare Bitmap jedoch eine elementare Bedeutung, da erst durch diese die im Barcode enthaltenen Daten für den Benutzer einen Sinn erhalten, ohne daß dazu techni-

sche Hilfsmittel eingesetzt werden müssen. Lediglich bei berechtigten Zweifeln an der Authentizität des Dokuments muß eine computerbasierte Signaturprüfung vorgenommen werden. Daher ermöglicht der zusätzliche Ausdruck der Bitmap in menschenlesbarer Form einen Umgang mit dem Dokument, der der Intuition des Benutzers sowie der klassischen Aktenführung entspricht.

Eine Manipulationsmöglichkeit besteht nun darin, die sichtbare Bitmap an entscheidenden Stellen zu verändern, ohne die gleiche Änderung auch an der im Barcode enthaltenen Bitmap vorzunehmen. Dieser Fall kann z.B. auftreten, wenn ein Dritter den Empfänger über den Inhalt der abgegebenen Willenserklärung täuschen will. Der Dritte kann zwar eine Änderung an der sichtbaren Bitmap mit modernen Bildverarbeitungsprogrammen leicht vorzunehmen, ohne Spuren zu hinterlassen. Eine entsprechende Änderung der im Barcode enthaltenen digital signierten Bitmap ist ihm jedoch ohne Kenntnis des geheimen Schlüssels des Unterzeichners nicht möglich bzw. würde bei der Signaturprüfung aufgrund der Ungültigkeit der Signatur sofort entdeckt werden. Auch der Unterzeichner könnte eine derartige Täuschung vornehmen wollen, z.B. um zunächst Rechte aus der angeblich signierten Willenserklärung und später gegebenenfalls Rechte aus der tatsächlich signierten Willenserklärung geltend zu machen.

Wird das Dokument auf die beschriebene Art manipuliert, enthält der Ausdruck zwei verschiedene Bitmaps. Die Signaturprüfung würde jedoch keinen Fehler anzeigen. Theoretisch könnte man anhand eines sorgfältigen Vergleichs zwischen dem Ausdruck und der auf dem Bildschirm angezeigten Bitmap alle Abweichungen feststellen, wobei die auf dem Bildschirm angezeigte Version letzten Endes gilt. Diese Situation ist jedoch unbefriedigend, da man eine derartige Überprüfung häufig nur

WO 01/09830

PCT/DE00/02606

22

sehr oberflächlich vornehmen wird, besonders dann wenn man annimmt, daß man dem Unterzeichner vertrauen kann. Es muß daher innerhalb des Verfahrens neben der reinen Signaturprüfung ein computerunterstützter Vergleich zwischen der eingescannten Bitmap und der aus dem eingescannten Barcode rekonstruierten Bitmap vorgenommen werden. Dabei ist zu berücksichtigen, daß Abweichungen zwischen beiden verschiedene Ursachen haben können:

1. Unvermeidliche Fehler in der Digital-Analog-Wandlung (d.h. beim Ausdrucken) und bei der Analog-Digital-Wandlung (d.h. beim Einscannen). Entscheidende Einflußgrößen sind hierbei die Qualität des Druckverfahrens, des Scanverfahrens und des verwendeten Papiers. Die dabei entstehenden Abweichungen sind aus Sicht des Benutzers irrelevant und sollten beim Vergleich durch intelligente Bildverarbeitungsmethoden so weit wie möglich eliminiert werden. Hierzu ist unter anderem eine gegebenenfalls beim Drucken und/oder Einscannen aufgetretene geometrische Verzerrung zu korrigieren. Daneben können sehr kleine Abweichungen, die z.B. nicht höher und breiter als zwei Pixel sind, im allgemeinen problemlos entfernt werden, ohne daß signifikante Abweichungen betroffen sind.

2. Abweichungen, die aus einer Änderung am Ausdruck resultieren und die aus Sicht des Überprüfenden unkritisch sind. Hierzu zählt z.B. ein vom Empfänger aufgebrachter Eingangsstempel.

3. Abweichungen, die aus einer Änderung am Ausdruck resultieren und die aus Sicht des Überprüfenden kritisch sind. Hierzu zählt z.B. ein vom Unterzeichner, vom Empfänger oder von einem Dritten von 1.000,- DM in 2.000,- DM geänderter Geldbetrag in einer Rechnung.

Die Abweichungen von Typ 2 und Typ 3 können im allgemeinen nicht automatisch unterschieden werden. Diese Abweichungen sind dem Überprüfenden daher in möglichst auffälliger Weise zu präsentieren. Dieser hat die endgültige Entscheidung zu treffen.

Obwohl das erfindungsgemäße Verfahren vorzugsweise dafür gedacht ist, im Rahmen elektronischer Transaktionen empfangene digital signierte Dokumente zu archivieren, sind auch sinnvolle Anwendungsmöglichkeiten denkbar, bei denen ein Ausdruck auf demselben Computersystem erfolgt, auf dem das Dokument erzeugt wird. Denkbar ist eine derartige Anwendung z.B. zur Dokumentation urheberrechtlicher Ansprüche, indem der Urheber eines Dokuments von einer Zertifizierungsstelle einen Zeitstempel für dieses Dokument erzeugen läßt. Bei dem Zeitstempel handelt es sich um ein elektronisches Dokument, gebildet aus dem Hash-Wert des Dokuments, dessen Vorliegen zu einem bestimmten Zeitpunkt bestätigt werden soll, und der zum Zeitpunkt des Signierens aktuellen Uhrzeit, das von der Zertifizierungsstelle digital signiert wird. Anstelle einer eigenen Signatur wird bei dieser Anwendung des Verfahrens der Zeitstempel archiviert. Später kann der Urheber jederzeit nachweisen, daß ihm das Dokument bereits zum durch den Zeitstempel dokumentierten Zeitpunkt vorlag. Sofern niemand einen früheren Zeitpunkt nachweisen kann, an dem das Dokument bereits öffentlich verfügbar war, sollte die Urheberschaft durch denjenigen angenommen werden, der das Dokument vorlegen kann.

Auch in allen Fällen, in denen die hohe Fälschungssicherheit digital signierter Daten ausgenutzt werden soll, z.B. bei behördlichen Dokumenten, kann das erfindungsgemäße Verfahren eingesetzt werden, auch wenn der Ausdruck persönlich an den Empfänger ausgehändigt wird. Hierbei ist vor allem von Vor-

teil, daß die hohe Fälschungssicherheit sehr kostengünstig zu erreichen ist. Dabei muß jedoch - wie allgemein bei digitalen Signaturverfahren - beachtet werden, daß das Verfahren nur einen Schutz vor Veränderungen von Dokumenten aber keinen Schutz vor Anfertigung identischer Kopien bietet.

Obwohl das erfindungsgemäße Verfahren optimal mit Papier und ähnlichen Datenträgern eingesetzt werden kann, sind Anwendungsfälle denkbar, bei denen ein stabilerer Datenträger verwendet werden soll, z.B. Kunststoff. Auch für diese Anwendungen eignet sich das erfindungsgemäße Verfahren, sofern für das jeweils benutzte Material ein Druckverfahren zur Verfügung steht, mit dessen Hilfe die Bitmap und der Barcode in akzeptabler Form aufgetragen werden können. Die einzige Beschränkung der zu bedruckenden Materialien liegt in der Bedingung, daß die aufgetragenen Daten sich korrekt durch optische Abtastung rekonstruieren lassen.

Erreichte Vorteile

Durch die erfindungsgemäßen Verfahren lassen sich Beweisstücke erzeugen und überprüfen, für die kein physischer Transport materieller Gegenstände notwendig ist. Dadurch lassen sich Zeit und Kosten sparen, die für den Transport herkömmlicher Dokumente notwendig wären.

Dennoch kann der Empfänger eines derartigen digital signierten Beweisstücks auf einfache und kostengünstige Weise einen materiellen Beweisgegenstand erzeugen, der über viele Jahre hinweg sicher und zuverlässig aufbewahrt werden kann. Durch die digitale Signatur ist dieser besser vor Manipulationen geschützt als herkömmliche Dokumente. Sofern alle zur Überprüfung der digitalen Signatur notwendigen Daten auf dem Ausdruck vorhanden sind, kann ein derartiges Dokument noch nach

Jahren überprüft werden, ohne daß ein Rückgriff auf andere Daten notwendig ist. Die Überprüfung der digitalen Signatur geht dabei schnell und einfach mittels eines auf dem erfindungsgemäßen Verfahren basierenden standardisierten Hardware- oder Software-Produkts.

5

Sollte eine Bestätigung der Signatur mißlingen, weil das Dokument verschmutzt oder beschädigt wurde, ist dennoch in vielen Fällen eine Bestätigung der Signatur prinzipiell möglich. Da sich bei genauem Hinsehen bzw. mit einem Vergrößerungsglas die Struktur der Bitmap erkennen läßt, ist theoretisch die manuelle Rekonstruktion der Bitmap möglich. Voraussetzung dafür ist, daß nur solche Teile der Bitmap fehlen oder beschädigt sind, die durch logisches Denken oder den Vergleich mit ähnlichen Dokumenten rekonstruiert werden können. Eine derartige manuelle Rekonstruktion ist zwar aufwendig, wird sich aber bei wichtigen Dokumenten lohnen. Die Möglichkeit einer manuellen Rekonstruktion von partiell beschädigten Beweisdaten trägt erheblich zur Sicherheit der archivierten Dokumente bei.

Der durch die digitale Signatur bestätigte Inhalt geht eindeutig aus der Bitmap auf einem Ausdruck hervor und ist auch ohne technische Hilfsmittel für jeden offensichtlich. Dadurch werden sinnentstellende oder verfälschende Manipulationen an der Darstellung eines digital signierten Dokuments effektiv verhindert.

Digitale Signaturen auf Papier scheinen einen Rückschritt darzustellen, da ein normalerweise zu vermeidender Medienbruch die Basis des Verfahrens bildet. Es können jedoch alle Vorteile elektronischer Transaktionen, wie z.B. schnelle und fehlerfreie Verarbeitung, genutzt werden. Allein zum Zweck der sicheren Aufbewahrung eines Beweisstücks wird beim Emp-

10

WO 01/09830

PCT/DE00/02606

26

fänger ein Dokument in Papierform erzeugt. Da es nur in Ausnahmefällen, z.B. bei Streitigkeiten, noch einmal benutzt wird, sind die Nachteile des Medienbruchs begrenzt. Die Vorteile wiegen diesen Nachteil bei weitem auf. Da sich für viele Privatpersonen - subjektiv und objektiv - die Beweissituation bei elektronischen Transaktionen bessert, wird eine große Hürde für die umfassende Nutzung elektronischer Transaktionen und die damit verbundenen Vorteile überwunden.

Durch die Verwendung einer Bitmap als dem zentralen Bestandteil der digital signierten Daten, ist eine hohe Flexibilität hinsichtlich des Inhalts und der graphischen Darstellung eines Dokuments gegeben. Eine Firma kann z.B. ihr Firmenlogo verwenden und damit das äußere Erscheinungsbild ihrer Geschäftsbriefe wahren. Für den Empfänger hat dies den Vorteil, daß sich seine Beweisstücke optisch besser unterscheiden und dadurch leichter wiederfinden lassen.

Ausführungsbeispiel

Im folgenden wird ein Ausführungsbeispiel der Erfindung anhand des elektronischen Versands einer Versicherungspolice über das Internet näher erläutert. Es zeigen:

Fig. 1 einen Ausdruck einer elektronisch übermittelten Versicherungspolice

Fig. 2 einen Detailausschnitt aus Fig. 1 (Rand der Bitmap)

Fig. 3 einen Detailausschnitt aus Fig. 1 (zweidimensionaler Barcode)

Erzeugung einer digital signierten Versicherungspolice in Papierform:

WO 01/09830

27

Ein Kunde füllt auf seinem Computer mit einem gewöhnlichen Web-Browser ein Antragsformular für eine Reisekrankenversicherung aus.

5

Das Antragsformular wird auf dem Computersystem der Versicherung automatisiert bearbeitet. Ist die Bearbeitung erfolgreich, wird ein elektronisches Dokument erzeugt, das die Versicherungspolice enthält.

10

Von diesem elektronischen Dokument wird erfindungsgemäß ein von der Versicherung digital signiertes elektronisches Dokument im PDF-Format erzeugt, das an den Kunden übermittelt wird.

15

Der Kunde empfängt die übermittelten Daten auf seinem Computer. Im Idealfall sind für ihn nur wenige Sekunden vergangen, seitdem er das Antragsformular abgesandt hat. Eine spezielle Software überprüft die Gültigkeit der digitalen Signatur und ob die im PDF-Dokument sichtbar enthaltene Bitmap mit der im Barcode enthaltenen Bitmap übereinstimmt.

20

5. Wenn diese Prüfung erfolgreich ist, bereitet die Software die Daten für einen Ausdruck auf und gibt sie auf einem angeschlossenen Drucker aus (siehe Fig. 1). Die Bitmap 1, die von einem Rahmen 2 umgeben ist, enthält sowohl Textbestandteile 3 als auch ein graphisches Element 4. Neben der Bitmap ist der zweidimensionale Barcode 5 auf dem Ausdruck enthalten. Der Rand 6 enthält dabei in regelmäßigen Abständen kleine Markierungen 7, die zur Korrektur etwaiger geometrischer Verzerrungen genutzt werden. Der Barcode besteht aus einem sogenannten Metasektor 8, der die Größe des Barcodes sowie weitere zum Decodieren benötigte Angaben enthält. Die Datenzone enthält

25

30

WO 01/09830

PCT/DE00/02606

28

sowohl Markierungen 9 als auch die eigentlichen Datenpunkte 10.

5 6. Findet der Kunde keine Fehler in der ausgestellten Versicherungspolice, kann er sie abheften und sicher aufbewahren. Zusätzlich kann er einen weiteren Ausdruck oder eine Kopie anfertigen, die er auf seiner Reise mitführen kann.

10 Die Verifikation der digitalen Signatur eines derart erzeugten Dokuments ist aus Sicht des Anwenders ebenso einfach:

Überprüfen eines digital signierten Dokuments in Papierform:

15 1. Das Dokument wird mit einem handelsüblichen Flachbett-Scanner oder einem ähnlichen Gerät eingescannt.

20 2. Mittels elektronischer Bildverarbeitung rekonstruiert eine spezielle Software die im Barcode enthaltene digitalen Daten, darunter die digital signierte Bitmap, die digitale Signatur und das Zertifikat der Versicherung.

25 3. Anhand der in Schritt 2 gewonnenen Daten wird die Signatur geprüft und im Erfolgsfall eine entsprechende Mitteilung ausgegeben und die in digitaler Form enthaltene Bitmap angezeigt.

30 4. Daneben werden die in Schritt 1 eingescannte Bitmap mit der in Schritt 2 rekonstruierten Bitmap verglichen und bei signifikanten Abweichungen dem Überprüfenden eine Mitteilung gemacht sowie die Abweichungen deutlich angezeigt. Basierend auf dieser Anzeige kann der Überprüfende die Entscheidung treffen, ob Manipulationen vorgenommen wurden oder nicht.

PCT/DE00/02606

WO 01/09830

29

Diese Überprüfung dauert in Abhängigkeit von den dabei eingesetzten Geräten einige Sekunden. Sollte z.B. die Versicherung bei Eintritt des Versicherungsfalls bestreiten, einen Versicherungsvertrag mit dem Kunden abgeschlossen zu haben, kann der Kunde jederzeit die digital signierte Versicherungspolice vorlegen und mit Hilfe des Verfahrens überprüfen lassen.

5

WO 01/09830

PCT/DE00/02606

30

5

PATENTANSPRÜCHE

10

1. Verfahren zur Darstellung digital signierter elektronischer Dokumente in gedruckter Form und zur Verifikation der Signatur aus der gedruckten Form, dadurch gekennzeichnet, daß zur Darstellung des Dokuments in gedruckter Form

15

- das elektronische Dokument in Form einer zweidimensionalen Matrix von Bildpunkten (Bitmap) dargestellt wird,

20

- Daten der zweidimensionalen Matrix von Bildpunkten (Bitmap) mittels des geheimen Schlüssels der digitalen Signatur verschlüsselt werden und

- die verschlüsselten Daten und die Bitmap in zumindest auch maschinenlesbarer Form gedruckt werden und

zur Verifikation der Signatur

25

- die gedruckte Form gescannt wird,

- aus dem durch das Scannen gewonnenen digitalen Abbild die zweidimensionale Matrix von Bildpunkten (Bitmap) und die digitale Signatur rekonstruiert wird, und

30

- die rekonstruierte Signatur anhand der rekonstruierten Matrix von Bildpunkten (Bitmap) verifiziert wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Bitmap gleichzeitig einen für Menschen lesbaren Ausdruck des digital signierten Dokuments darstellt und gleichzeitig maschinenlesbar ist.

5 3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das digital signierte Dokument parallel in für Menschen lesbarer und maschinenlesbarer Form ausgedruckt wird und bei der Verifikation der Signatur die maschinenlesbare Form eingescannt
10 und damit die ursprünglichen Daten rekonstruiert werden und die Daten der Bitmap aus den ursprünglichen Daten wieder hergestellt werden und sodann die Daten der wieder hergestellten Bitmap mit dem in für Menschen lesbarer Form ausgedruckten Dokument verglichen werden.

15 4. Verfahren nach Anspruch 3, dadurch gekennzeichnet, daß der Vergleich automatisch mittels spezieller Bildverarbeitungsverfahren erfolgt, die signifikante Abweichungen anzeigen.

20 5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß die Daten der Bitmap vor der Verschlüsselung komprimiert und vor der Verifikation dekomprimiert werden.

25 6. Verfahren nach Anspruch 3 oder 4, dadurch gekennzeichnet, daß der Ausdruck in maschinenlesbarer Form als zweidimensionaler Barcode erfolgt.

30 7. Verfahren nach Anspruch 6, dadurch gekennzeichnet, daß der für den Menschen lesbare Ausdruck des Bitmap mit einem Rahmen mit in regelmäßigem Abstand angeordneten Markierungen umgeben ist.


WO 01/09830

1/5

PCT/DE00/02606

Fig.1

Beispiel-Versicherungen AG



Beispielhausen, 1. Januar 2001

Auslandsreise-Krankenversicherung

Sehr geehrter Herr Mustermann,

hiermit senden wir Ihnen die Versicherungsunterlagen für Ihre Reisekrankenversicherung zu. Bitte machen Sie einen Ausdruck von diesem Dokument und verwahren ihn sorgfältig. Er ist Ihr Versicherungsnachweis.

Versicherungsnummer: RK45 863 221 009
Versicherungsnehmer: Matthias Mustermann
Geburtsdatum: 01.01.1970
Anschrift: Hauptstraße 10
12345 Musterstadt

Tarif: Reisekrankenversicherung RK 45
Versichert sind alle Auslandsaufenthalte des Versicherungsnehmers im Versicherungszeitraum mit einer Dauer von jeweils maximal 45 Tagen.

Versicherungszeitraum: 01.01.2001 - 31.12.2001
Versicherungsprämie: 20,00 DM (10,23 EUR)

Die Versicherungsprämie wird in den nächsten Tagen von Ihrem Konto abgebucht.

Seite 1 von 1

1 5

Dieses Dokument ist digital signiert.

WO 01/09830

2/5

PCT/DE00/02606

Fig. 2

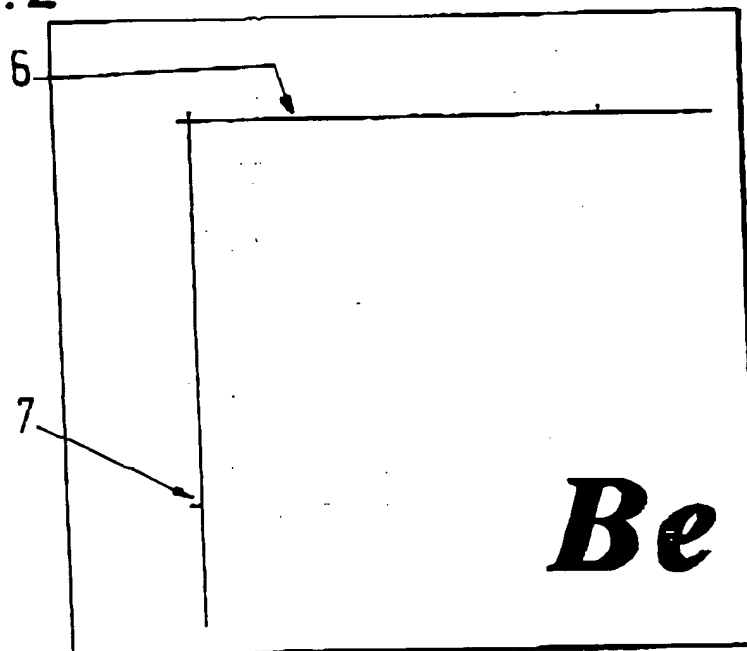
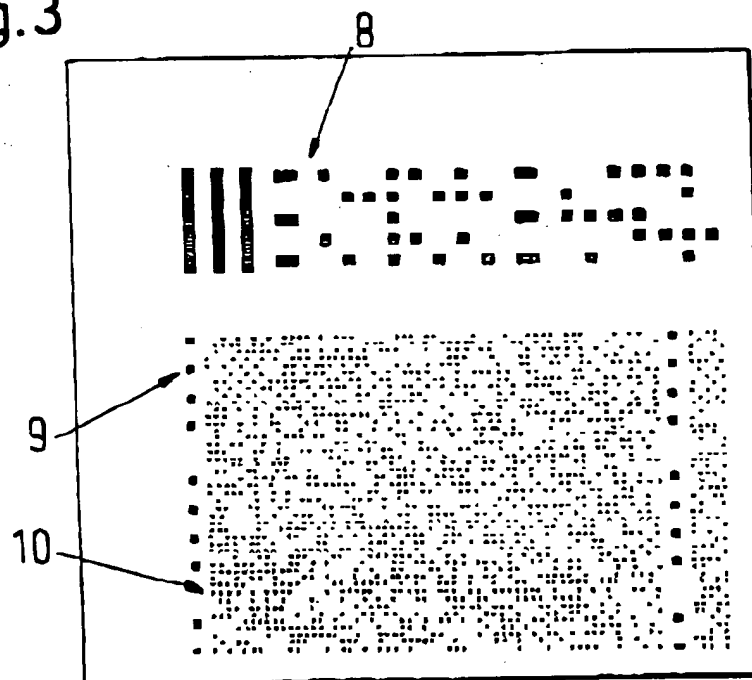


Fig. 3



WO 01/09830

3/5

PCT/DE00/02606

Fig.4

Herrn
Matthias Mustermann
Mustergasse 1
20000 Musterhausen

Musterstadt, 1. März 2000

RECHNUNG

Sehr geehrter Herr Mustermann,

für die Lieferung von Software berechnen
wir Ihnen:

Textverarbeitungsprogramm	171,55
+16% Mehrwertsteuer	<u>27,45</u>
Bruttobetrag	<u>199,00</u>

Mit freundlichen Grüßen

ABC Softwareversand

WO 01/09830

4/5

PCT/DE00/02606

Fig.5

Herrn
Matthias Mustermann
Müstergasse 1
20000 Musterhausen

Musterstadt, 1. März 2000

RECHNUNG

Sehr geehrter Herr Mustermann,
für die Lieferung von Software berechnen
wir Ihnen:

Textverarbeitungsprogramm
+16% Mehrwertsteuer

1.033,62
165,38

Bruttobetrag

1.199,00

Mit freundlichen Grüßen

ABC Softwareversand

Eingegangen:

03.03.2000

WO 01/09830

5/5

PCT/DE00/02606

Fig.6

Herrn Matthias Mustermann Mustergasse 1 20000 Musterhausen	
Musterstadt, 1. März 2000	
<u>RECHNUNG</u>	
Sehr geehrter Herr Mustermann, für die Lieferung von Software berechnen wir Ihnen:	
Textverarbeitungsprogramm	1.033,62
+16% Mehrwertsteuer	165,38
Bruttobetrag	<u>1.199,00</u>
Mit freundlichen Grüßen	
ABC Softwareversand	<div>Eingegangen: 03.03.2000</div>

INTERNATIONAL SEARCH REPORT

Intern Application No

PCT/DE 00/02606

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06K19/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, INSPEC, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category * Citation of document, with indication, where appropriate, of the relevant passages

Relevant to claim No.

X

WO 96 15621 A (SARAT JEAN MARC ;BOUTILLIER
JEAN YVES (FR); GEMPLUS CARD INT (FR))
23 May 1996 (1996-05-23)
page 2, line 5 -page 4, line 2; claims
1-3,7; figures 1,2
page 10, line 9-27; claims 1-3,7; figures
1,2

1-3,5-7

X

EP 0 676 877 A (IBM)
11 October 1995 (1995-10-11)
page 2, line 36-54
page 4, column 7, line 35

1-3

X

EP 0 639 919 A (POSTE ;FRANCE TELECOM
(FR)) 22 February 1995 (1995-02-22)
column 5, line 54 -column 11, line 23;
figure 1

1,2

Y

5

-/--

☒

Further documents are listed in the continuation of box C.

☒

Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

G document member of the same patent family

Date of the actual completion of the international search

23 November 2000

Date of mailing of the international search report

30/11/2000

Name and mailing address of the ISA

European Patent Office, P.B. 5618 Patenzahn 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo.nl
Fax: (+31-70) 340-3016

Authorized officer

Schauler, M

INTERNATIONAL SEARCH REPORT

Intern Application No

PCT/DE 00/02606

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 321 749 A (VIRGA RICHARD) 14 June 1994 (1994-06-14) abstract; figure 10	5
A	EP 0 889 448 A (PITNEY BOWES) 7 January 1999 (1999-01-07) column 3, line 9 -column 4, line 53; claims 10,11	1-4,6

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intern. Application No

PCT/DE 00/02606

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 9615621	A	23-05-1996	FR 2726953 A CA 2206135 A DE 69514004 D DE 69514004 T EP 0792553 A ES 2144152 T JP 9512114 T	15-05-1996 23-05-1996 20-01-2000 27-04-2000 03-09-1997 01-06-2000 02-12-1997
EP 0676877	A	11-10-1995	GB 2288476 A US 5912974 A	18-10-1995 15-06-1999
EP 0639919	A	22-02-1995	FR 2709218 A DE 69417493 D DE 69417493 T JP 7177278 A US 5530755 A	24-02-1995 06-05-1999 21-10-1999 14-07-1995 25-06-1996
US 5321749	A	14-06-1994	AU 5135193 A WO 9407326 A US 5398283 A	12-04-1994 31-03-1994 14-03-1995
EP 0889448	A	07-01-1999	NONE	

PCT/DE 00/02606

Seite 1 von 2

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/DE 00/02606

C. (Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Beitr. Anspruch Nr.
Y	US 5 321 749 A (VIRGA RICHARD) 14. Juni 1994 (1994-06-14) Zusammenfassung; Abbildung 10	5
A	EP 0 889 448 A (PITNEY BOWES) 7. Januar 1999 (1999-01-07) Spalte 3, Zeile 9 - Spalte 4, Zeile 53; Ansprüche 10,11	1-4,6

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/DE 00/02606

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
WO 9615621 A	23-05-1996	FR 2726953 A	15-05-1996
		CA 2206135 A	23-05-1996
		DE 69514004 D	20-01-2000
		DE 69514004 T	27-04-2000
		EP 0792553 A	03-09-1997
		ES 2144152 T	01-06-2000
		JP 9512114 T	02-12-1997
EP 0676877 A	11-10-1995	GB 2288476 A	18-10-1995
		US 5912974 A	15-06-1999
EP 0639919 A	22-02-1995	FR 2709218 A	24-02-1995
		DE 69417493 D	06-05-1999
		DE 69417493 T	21-10-1999
		JP 7177278 A	14-07-1995
		US 5530755 A	25-06-1996
US 5321749 A	14-06-1994	AU 5135193 A	12-04-1994
		WO 9407326 A	31-03-1994
		US 5398283 A	14-03-1995
EP 0889448 A	07-01-1999	KEINE	